demo

Report generated by Nessus™ Sat, 21 Jan 2023 12:27:16 PKT

Vulnerabilities by Plugin

Vulnerabilities by Plugin

58987 (1) - PHP Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF	IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2022/12/07

Plugin Output

testphp.vulnweb.com (tcp/80/www)

```
  Source               : X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
```

```
    Installed version   : 5.6.40-38+ubuntu20.04.1+deb.sury.org+1
    End of support date : 2018/12/31
    Announcement        : http://php.net/supported-versions.php
    Supported versions  : 8.0.x / 8.1.x
```

10107 (1) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

testphp.vulnweb.com (tcp/80/www)

```
The remote web server type is :

nginx/1.19.0
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

testphp.vulnweb.com (udp/0)

```
For your information, here is the traceroute from 192.168.88.129 to 44.228.249.3 :
192.168.88.129
192.168.88.2
44.228.249.3

Hop Count: 2
```

11153 (1) - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

Plugin Output

testphp.vulnweb.com (tcp/80/www)

```
A web server seems to be running on this port.
```

11219 (1) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/11/30

Plugin Output

testphp.vulnweb.com (tcp/80/www)

```
Port 80/tcp was found to be open
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

testphp.vulnweb.com (tcp/0)

```

Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP


The remote host is running CISCO PIX 7.0
```

12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

testphp.vulnweb.com (tcp/0)

```
44.228.249.3 resolves as ec2-44-228-249-3.us-west-2.compute.amazonaws.com.
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2022/06/09

Plugin Output

testphp.vulnweb.com (tcp/0)

```
Information about this scan :

Nessus version : 10.4.2
Nessus build : 20093
Plugin feed version : 202301121947
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian9-x86-64
Scan type : Normal
Scan name : demo
Scan policy used : Basic Network Scan
Scanner IP : 192.168.88.129
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 367.910 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2023/1/21 12:12 PKT
Scan duration : 890 sec
```

24260 (1) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

testphp.vulnweb.com (tcp/80/www)

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: nginx/1.19.0
  Date: Sat, 21 Jan 2023 07:21:45 GMT
  Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
  Connection: keep-alive
  X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
 codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
```

```
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306"
 height="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
      <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
<td align="left">
<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
 href="artists.php">artists
 [...]
```

32318 (1) - Web Site Cross-Domain Policy File Detection

Synopsis

The remote web server contains a 'crossdomain.xml' file.

Description

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

See Also

http://www.nessus.org/u?8a58aa76

http://kb2.adobe.com/cps/142/tn_14213.html

http://www.nessus.org/u?74a6a9a5

http://www.nessus.org/u?acb70df2

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.

Risk Factor

None

Plugin Information

Published: 2008/05/15, Modified: 2022/04/11

Plugin Output

testphp.vulnweb.com (tcp/80/www)

```
Nessus was able to obtain a cross-domain policy file from the remote
host using the following URL :

  http://testphp.vulnweb.com/crossdomain.xml
```

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2022/11/30

Plugin Output

testphp.vulnweb.com (tcp/0)

```

The remote operating system matched the following CPE :

  cpe:/o:cisco:pix_firewall:7.0 -> Cisco PIX Firewall Software

Following application CPE's matched on the remote system :

  cpe:/a:igor_sysoev:nginx:1.19.0 -> Nginx
  cpe:/a:nginx:nginx:1.19.0 -> Nginx
  cpe:/a:php:php:5.6.40 -> PHP PHP
  cpe:/a:php:php:5.6.40-38+ubuntu20.04.1+deb.sury.org+1 -> PHP PHP
```

48243 (1) - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2022/10/12

Plugin Output

testphp.vulnweb.com (tcp/80/www)

```
Nessus was able to identify the following PHP version information :

  Version : 5.6.40-38+ubuntu20.04.1+deb.sury.org+1
  Source  : X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

testphp.vulnweb.com (tcp/0)

```
Remote device type : firewall
Confidence level : 70
```

72427 (1) - Web Site Client Access Policy File Detection

Synopsis

The remote web server contains a 'clientaccesspolicy.xml' file.

Description

The remote web server contains a client access policy file. This is a simple XML file used by Microsoft Silverlight to allow access to services that reside outside the exact web domain from which a Silverlight control originated.

See Also

http://www.nessus.org/u?a4eeeaa2

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery or other attacks against the web server.

Risk Factor

None

Plugin Information

Published: 2014/02/11, Modified: 2021/01/19

Plugin Output

testphp.vulnweb.com (tcp/80/www)

```
Nessus was able to obtain a client access policy file from the
remote host at the following URL :

  GET /clientaccesspolicy.xml HTTP/1.1
Host: testphp.vulnweb.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

106375 (1) - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2021/04/07

Plugin Output

testphp.vulnweb.com (tcp/80/www)

```
URL     : http://testphp.vulnweb.com/
Version : 1.19.0
source  : Server: nginx/1.19.0
```

166602 (1) - Asset Attribute: Fully Qualified Domain Name (FQDN)

Synopsis

Report Fully Qualified Domain Name (FQDN) for the remote host.

Description

Report Fully Qualified Domain Name (FQDN) for the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/10/27, Modified: 2022/10/27

Plugin Output

testphp.vulnweb.com (tcp/0)

```
The FQDN for the remote host has been determined to be:

  FQDN       : ec2-44-228-249-3.us-west-2.compute.amazonaws.com
  Confidence : 100
  Resolves   : True
  Method     : rDNS Lookup: IP Address

Another possible FQDN was also detected:
```